



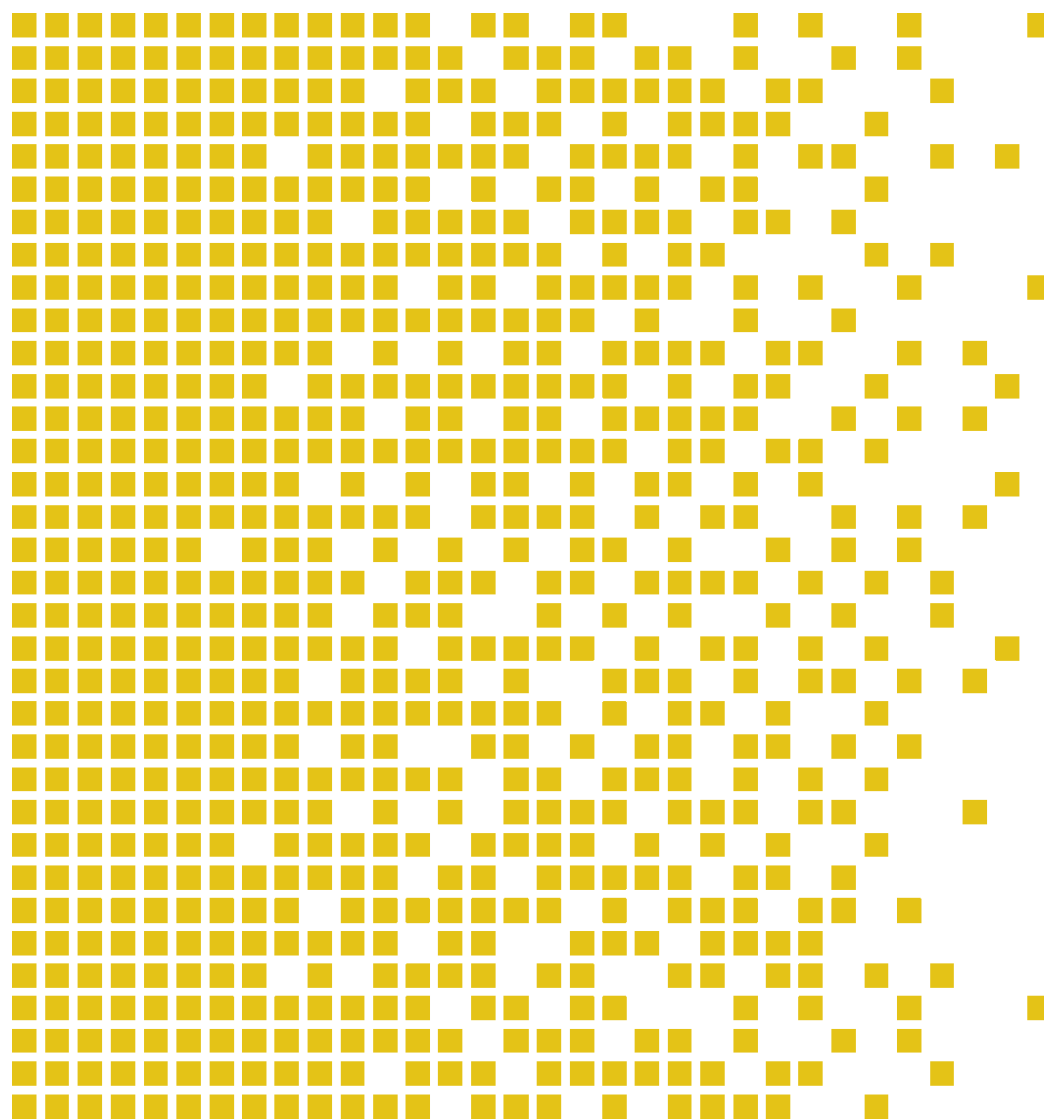
SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-034 CR Certification Report

Issue 1.0 16 December 2011

ZXUN USPP Universal Subscriber Profile Platform v. 4.11.10



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

**ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN
THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

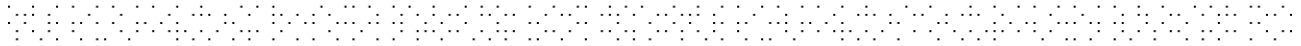
The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

* Mutual Recognition under the CC recognition arrangement applies to EAL 2 but not to ALC_FLR.2.



Contents

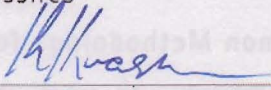

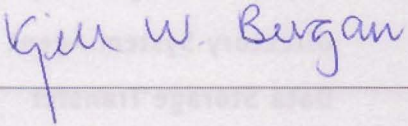
1	Certification Statement	5
2	Abbreviations	6
3	References	7
4	Executive Summary	9
4.1	Introduction	9
4.2	Evaluated Product	9
4.3	TOE scope	9
4.4	Protection Profile Conformance	9
4.5	Assurance Level	9
4.6	Security Policy	9
4.7	Security Claims	10
4.8	Threats Countered	10
4.9	Threats Countered by the TOE's environment	10
4.10	Threats and Attacks not Countered	10
4.11	Environmental Assumptions and Dependencies	10
4.12	IT Security Objectives	11
4.13	Non-IT Security Objectives	11
4.14	Security Functional Requirements	12
4.15	Security Function Policy	13
4.16	Evaluation Conduct	13
4.17	General Points	14
5	Evaluation Findings	15
5.1	Introduction	15
5.2	Delivery	16
5.3	Installation and Guidance Documentation	16
5.4	Misuse	16
5.5	Vulnerability Analysis	16
5.6	Developer's Tests	16
5.7	Evaluators' Tests	16
6	Evaluation Outcome	17
6.1	Certification Result	17
6.2	Recommendations	17
	Annex A: Evaluated Configuration	19
	TOE Identification	19
	TOE Documentation	19
	TOE Configuration	20
	Environmental Configuration	21



1 Certification Statement

ZTE Corporation ZXUN USPP Universal Subscriber Profile Platform is a home location register for mobile phone subscribers.

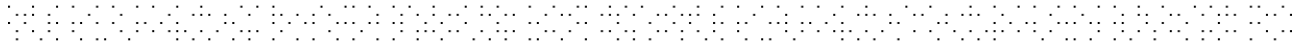
ZXUN USPP Universal Subscriber Profile Platform version 4.11.10 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes
Certifier	
Quality Assurance	Lars Borgos
Quality Assurance	
Approved	Kjell W. Bergan
Head of SERTIT	
Date approved	16 December 2011

2 Abbreviations

AAA	Authentication, Authorization, Accounting
BOSS	Business Operation Support System
BSS	Business Support Systems
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CDMA	Code Division Multiple Access
CDMA2000 1x/EV-DO	CDMA2000 1x evolution data-only
DAS	Data accessing and synchronization network
DSA	Directory System Agent
DST	Data Storage Transfer
EAL	Evaluation Assurance Level
EMS	Network Element Management System
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
FE	Front End subsystem
GPRS	General Packet Radio Service
GSM	Global System of Mobile Communication
IMS	IP Multimedia System
L3 switch	Layer 3 switch
LTE	Long Term Evolution
MSC	Mobile Switching Centre
NE	Network elements in the core network
NM VLAN	Network Management VLAN
OMC VLAN	Operator-maintained VLAN
OMM	Operational Maintenance Module

OSS	Operations Support Systems
POC	Point of Contact
SERTIT	Norwegian Certification Authority for IT Security
SGSN	Serving GPRS support node
SMS	Short Message Service
SPM	Security Policy Model
ST	Security Target
SN	Signalling Network
SS7	Signalling System No 7
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UDS	Universal Directory Server
UMTS	Universal Mobile Telecommunications System
USPP	Universal Subscriber Profile Platform
VLAN	Virtual Local Area Network
WIMAX	Worldwide Interoperability for Microwave Access
QP	Qualified Participant



3 References

- [1] Security Target, ZTE Corporation, ZTE ZXUN USPP Universal Subscriber Profile Platform 4.11.10, version 1.1, 13 October 2011.
- [2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.
- [3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.
- [4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.
- [5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.
- [6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.
- [7] Evaluation Technical Report Common Criteria EAL2+ Evaluation of ZTE ZXUN USPP Universal Subscriber Profile Platform, version 1.1, 14 December 2011.
- [8] ZXUN USPP Common Criteria Security Evaluation – Certified Configuration R1.2
- [9] Software Installation Guide (R1.3)
- [10] General Operation Guide (OMM Volume) (R1.3)
- [11] Hardware Installation Guide (R1.1)

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZXUN USPP Universal Subscriber Profile Platform version 4.11.10 to the Sponsor, ZTE Corporation, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was ZXUN USPP Universal Subscriber Profile Platform version 4.11.10.

This product is also described in this report as the Target of Evaluation (TOE). The developer was ZTE Corporation.

The TOE is a next generation home location register (HLR). It is a central database of a mobile core network which contains details of mobile phone subscribers that are authorized to use the mobile core network.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.3.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL 2 augmented with ALC_FLR.2 Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in the ST[1], chapter 3.1.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

The Security Target introduces one extended component: FAU_GEN.3 Simplified audit data generation. This component is a simplified version of FAU_GEN.1 and is therefore a suitable member of the FAU_GEN family. It was added to remove the need to log start and stop of auditing and to simplify the requirement.

4.8 Threats Countered

- TA.ROGUE_USER_* tries to gain access to the subscribers' authentication data that is outside their authorisation
- TA.ROGUE_USER_* performs actions on the TOE that he is authorized to do, but these are undesirable and it cannot be shown that this user was responsible
- TA.ROGUE_SUB seeking to gain more access than he is entitled, to access and modify subscribers' data than that he is allowed to
- TA.NETWORK_NM, TA.OMC_VLAN, or TA.STORAGE_VLAN tries to gain unauthorized access to the TOE and is able to perform actions on the TOE or access subscribers' authentication data of the TOE
- TA.NETWORK_NM, TA.OMC_VLAN, or TA.STORAGE_VLAN is able to listen in/modify to access the subscribers' authentication data
- TA.ROGUE_SUB tries to overload the TOE to perform DoS attack
- TA.PHYSICAL gains physical access to the TOE (either client or server) and is able to use its functionality

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

It is assumed that if a subscriber wants to modify his own allowed service, he has be firstly identified and authorised by:

- VLR in the GSM network for the GSM subscribers
- VLR/SGSN in the UMTS network for the UMTS subscribers
- MSC/VLR in the CDMA network

4.12 IT Security Objectives

- The TOE shall ensure that all the sensitive subscribers' authentication data (such as Ki and Opc in the GSM network) are encrypted while stored and transmitted between USPPs
- The OMM shall support OMM user authentication, allowing the OMM to accept/reject users based on username/password and a configurable subset of IP address and time of login
- The Provisioning server shall support provisioning user authentication, allowing the Provisioning server to accept/reject provisioning users based on username/password and a configurable subset of IP address and time of login
- The TOE shall identify NEs in the GSM, UMTS, IMS, LTE, and CDMA network before providing subscribers' authentication data to these mobile networks
- The TOE shall support subscriber authentication for the cdma2000 1x/EV-DO, GPRS/UMTS network, WiMAX network, fixed broadband network, and 3GPP network, allowing the TOE to accept/reject subscribers based on NAI and IMSI
- The TOE shall support a flexible role-based authorisation framework with predefined and customizable roles. These roles can use the OMM server to manage the TOE or use the Provisioning functionality of the TOE. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this
- The TOE shall support logging and auditing of user actions
- The TOE shall
 - Prohibit users with no OMM privilege to login the OMM Web Client and access the OMM functionalities
 - Prohibit users with no Provisioning privilege to login the Provisioning Web Client or Provisioning server using the BOSS server to access the Provisioning functionalities
- The TOE shall:
 - protect communication between the OMM server and the EMS against masquerading, disclosure and modification
 - protect communication between the Provisioning web client and the Provisioning server against masquerading, disclosure and modification
 - protect communication between the OMM web client and the OMM server against disclosure and modification
- The TOE shall allow authorised subscribers limited access to their own subscriber data, to manage standard-defined services, based on standards
- The TOE shall provide load control mechanism to handle overload traffic, and ensure system reliability, to prevent DoS type attack

4.13 Non-IT Security Objectives

- The operator shall ensure that workstations that host one of the Clients are only connected to the OMC VLAN of the TOE, and protected from physical and logical attacks that would allow attackers to subsequently:
 - Disclose passwords or other sensitive information

- Hijack the client
- Execute man-in-the-middle attacks between client and TOE or similar attacks
- The operator shall maintain the following separated private network:
 - Storage VLAN
 - OMC VLAN
 - BOSS network
 - Data Accessing & Synchronization network
 - Network Management network
 - Signalling network
- The operator shall configure the Secure Network to:
 - protect communication between the TOE and other USPPs against masquerading, disclosure, and modification
 - protect communication between the TOE and BOSS against masquerading, disclosure, and modification
 - protect communication between the TOE and other NEs in the signaling network against masquerading, disclosure, and modification
- The operator shall ensure that the USPP shall be protected from physical attacks
- The EMS shall supply the TOE with reliable time
- The operator shall ensure that OMM, Provisioning and BOSS roles are only assigned to users that are sufficiently trustworthy and sufficiently trained to fulfill those roles
- The operator shall ensure that the EMS, BOSS server, all the NEs in the signalling network (such as MSCS/VLR in GSM and UMTS network, S-CSF in IMS network, and MME in the LTE network), and other USPPs are trusted, and will not be used to attack the TOE. The operator shall configure the L3 switch to block all traffic from/to the external network except for :
 - Selected traffic between EMS and OMM server
 - Selected traffic between BOSS and Provisioning server
 - Selected traffic between USPP and other USPPs
- The subscribers shall be authenticated and authorised by
 - VLR in the GSM network for the GSM subscriber
 - VLR/SGSN in the UMTS network for the UMTS subscribers
 - MSC/VLR in the CDMA network for the CDMA subscribersbefore they can access and modify his own allowed services (defined in 3GPP TS 22.004, Table 4.1 and 3GPP2 S.R0006)

4.14 Security Functional Requirements

- FIA_UID.2 User identification before any action
- FIA_UAU.2 User authentication before any action
- FTA_SSL.3 TSF-initiated termination
- FIA_AFL.1 Authentication failure handling
- FIA_SOS.1 Verification of secrets
- FTA_MCS.1 Basic limitation on multiple concurrent sessions

- FMT_SMR.1 Security roles
- FDP_ACC.2 Complete access control
- FAU_GEN.3 Simplified audit data generation
- FAU_SAR.1 Audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FDP_ITT.1 Basic internal transfer protection
- FDP_UCT.1 Basic data exchange confidentiality
- FTP_ITC.1 Inter-TSF trusted channel
- FRU_PRS.1 Limited priority of service
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FMT_SMF.1 Specification of Management Functions

4.15 Security Function Policy

The TOE has the following general functionalities:

- Telecommunications functionality:
 - It maintains the user subscription information and provides interface for operators to manage the subscription information.
 - It provides subscriber data to various mobile core network to allow these mobile core network to authorise the subscribers to use the service of the mobile network according to their information.
 - It can act as AAA server in various packet data service mobile network and fixed broadband network.
 - It interacts with the signalling network to provide routing information for mobile terminal (MT) calls and short message service (SMS).
- Management functionality:
 - Manage and configure the TOE
 - Interact with EMS to be managed and configured

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 14.12.2011. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3. These classes comprise the EAL 2 assurance package augmented with ALC_FLR.2

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the Operational User Guidance[8][9][10][11] documents provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Developers should follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The evaluators assessed all possible vulnerabilities found during evaluation of the classes. This resulted in a list of possible vulnerabilities to be tested.

The evaluators assessed which potential vulnerabilities were already tested by the developer and assessed the results except those tests from [ATE IND AVA].

The remaining potential vulnerabilities were tested by Brightsight on the final version of the TOE at the premises of ZTE, Nanjing, China through remote terminal clients in September 2011.

5.6 Developer's Tests

The developer test effort is considered already fairly complete. Any major missing features reported by the evaluators have been added to the developer test set. And the developer integrated tests for similar functionality into a bigger test case. Nevertheless the evaluator has defined 19 additional tests for the OMM, Provisioning, BOSS and FE server subsystems as the evaluator's independent tests and penetration tests.

5.7 Evaluators' Tests

In September 2011, tests on USPP V4.11.10 version of the TOE at the premise of ZTE in Nanjing, China were done on site and through the remote terminal client. During the tests the evaluator has extended some tests to create more variety in the tests.

For independent testing, the evaluator has repeated 12 of the 55 developer's tests. For each of the TSFI available one test is performed.

6 Evaluation Outcome

6.1 Certification Result

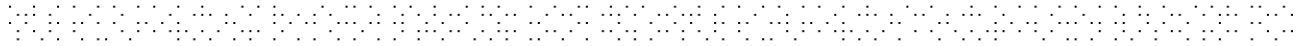
After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that ZXUN USPP Universal Subscriber Profile Platform version 4.11.10 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of ZXUN USPP Universal Subscriber Profile Platform version 4.11.10 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 "TOE Scope" and Section 0 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.



Annex A: Evaluated Configuration

TOE Identification

The TOE consists of the following:

Type		Name and version
Hardware	OMM Server	1x DPBX1 ¹
	Provisioning	1x DPBB2
	FE	
	DSA	1x DPBB1
	DST	
	Disk array	Fujitsu DX60
Software	OMM Server	ZTE CGS Linux V3.02.00_P01/32bit USPP V4.11.10 Apache 2.2.3 (with patch listed in appendix A installed)
	Provisioning	USPP V4.11.10
	DSA	USPP V4.11.10
	DST	ZTE CGS Linux V3.02.00_P01/64bit USPP V4.11.10
	FE	USPP V4.11.10
	Disk array	Oracle 10g se

The Provisioning, DSA, DST, FE may consist of more boards (DPBX1, DPBB1, and DPBB2). More board gives identical functionally, but provide better performance and more capacity.

TOE Documentation

The developer's documents evaluated were:

- [a] ZXUN USPP FSP-TDS V1.0
- [b] ZXUN USPP Security Architecture / Guidance V1.1
- [c] ZXUN USPP DEL.1, CMC.2, CMS.2, FLR.2 documentation V2.0
- [d] ZXUN USPP Common Criteria Security Evaluation – Certified Configuration R1.2
- [e] Software Installation Guide (R1.3)
- [f] General Operation Guide (OMM Volume) (R1.3)

¹ These are boards built by ZTE. The last two digits are the version number

[g] Hardware Installation Guide (R1.1)

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

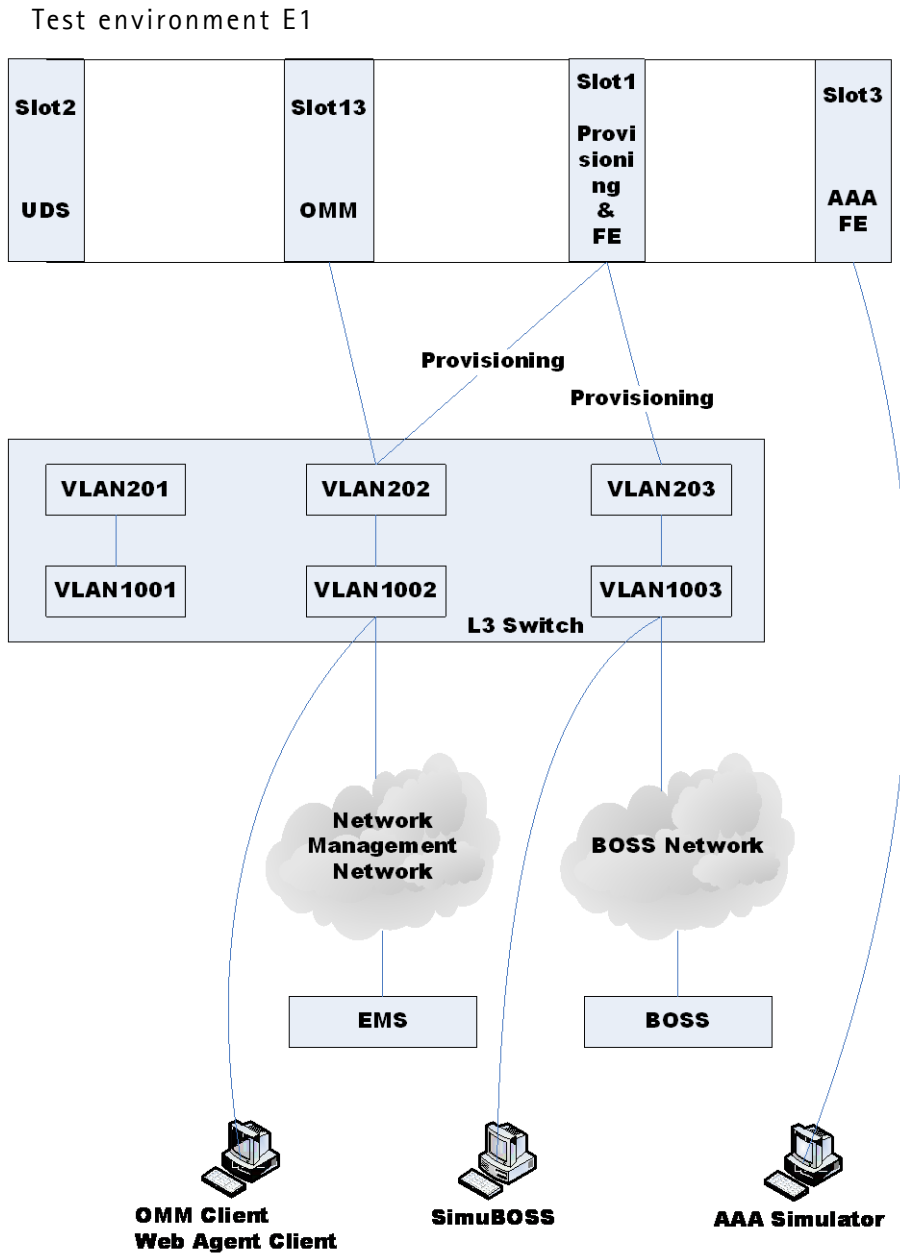
TOE Configuration

The following configuration was used for testing:

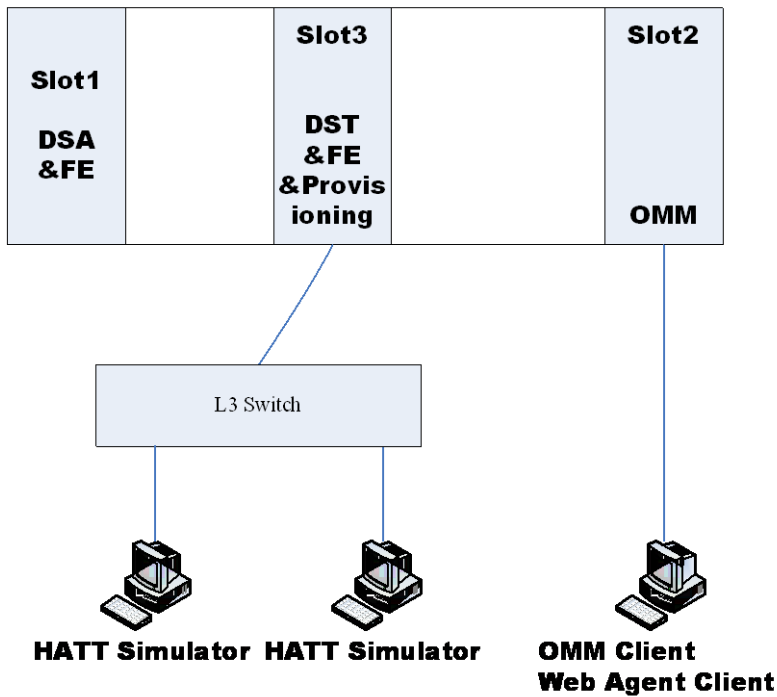
HARDWARE	DPBX1 (for the OMM server) DPBB2 (for the Provisioning) DPBB1 (for the FE and DSA/DST) Fujitsu DX60 (for the Disk Array)
SOFTWARE	OMM Server (USPP V4.11.10) Provisioning (USPP V4.11.10) DSA/DST (USPP V4.11.10) FE (USPP V4.11.10) Oracle 10g se (Disk Array)

Environmental Configuration

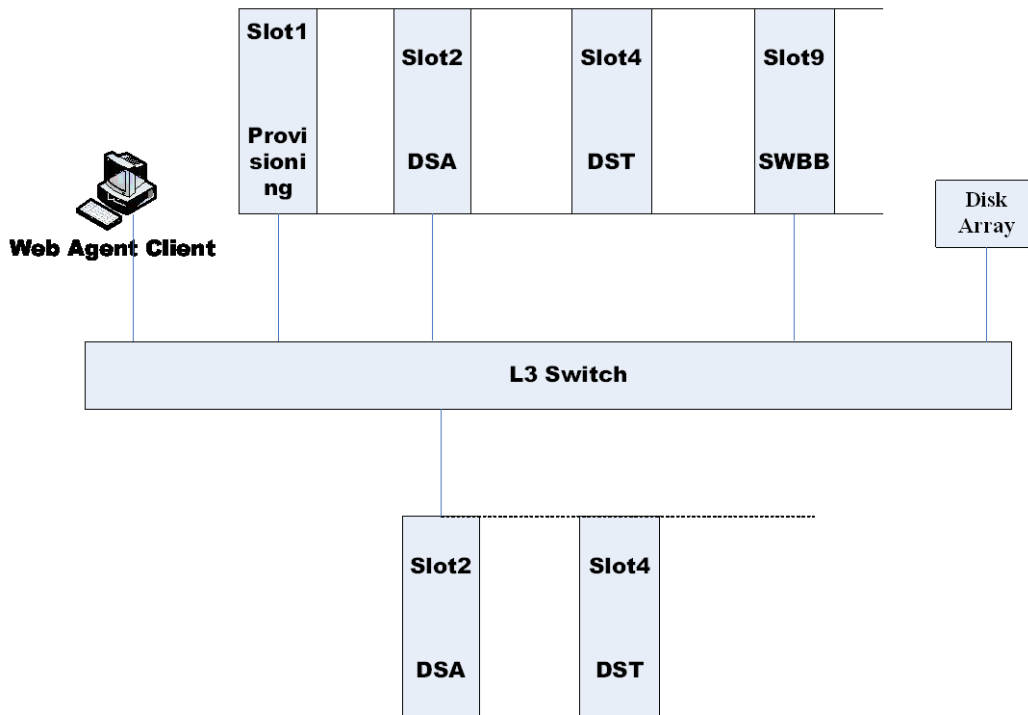
The TOE is tested in the following test set-ups:



Test environment E2



Test environment E3



Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Product Manufacturer: ZTE Corporation

Product Name: ZXUN USPP Universal Subscriber Profile Platform

Type of Product: Home location register for mobile phone subscribers

Version and Release Numbers: Version 4.11.10

Assurance Package: EAL 2 augmented with ALC_FLR.2

Evaluation Criteria: Common Criteria version 3.1R3 (ISO/IEC 15408)

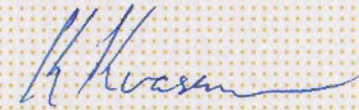
Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Certification Body: SERTIT

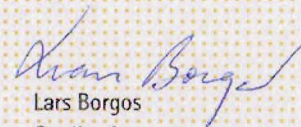
Certification Report Identifier: SERTIT-034 CR, issue 1.0, 16 December 2011

Certificate Identifier: SERTIT-034-C

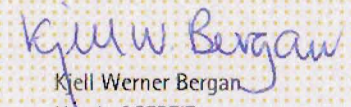
Date Issued: 16 December 2011



Kjartan Jæger Kvassnes
Certifier



Lars Borgos
Quality Assurance



Kjell Werner Bergan
Head of SERTIT



SERTIT

Norwegian Certification Authority for IT Security

